UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/521,424	03/08/2000	Satoru Wakao	35.G2550	1497

5514 7590 12/17/2003

FITZPATRICK CELLA HARPER & SCINTO
30 ROCKEFELLER PLAZA
NEW YORK, NY 10112

EXAMINER	
HO, THOMAS M	
ART UNIT	**PAPER NUMBER**
2134	8

DATE MAILED: 12/17/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/521,424	**Applicant(s)** WAKAO ET AL.	
	Examiner Thomas M Ho	**Art Unit** 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 March 2000*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-42* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-42* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)□ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) □ The translation of the foreign language provisional application has been received.

14)□ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____.

4) □ Interview Summary (PTO-413) Paper No(s). _____.

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: .

DETAILED ACTION

1. The preliminary amendment of 5/31/2000 has been received and entered.

2. Claims 1- 42 are pending.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate

A method for operating a portable authorization device paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims are 1-6, 8-10, 12-17, 20-26, 28-34, 37-42 rejected under 35 U.S.C. 102(b) as being unpatentable over Friedman, US Patent 5,499,294.

In reference to claim 1:

Friedman discloses an image processing apparatus comprising:

- calculation means for performing a predetermined calculation using a digital image and confidential information, where the predetermined calculation is a digital hash of the image (Column 4, lines 34-36), and the confidential information is textual information added to the image including a unique image sequence number and the GPS location at which the image was taken. (Column 4, lines 55-66) & (Column 9, lines 15-28)

- generation means for generating signature data, using an output of said calculation means, for use in detecting the integrity of the digital image. (Column 4, lines 37-46)

In reference to claim 2:

Friedman discloses an image processing apparatus wherein an inverted calculation of the predetermined calculation is possible, predetermined calculation is the hash and the inverted calculation generates the hash by inverting the encryption previously done. (Column 4, lines 47-54)

In reference to claim 3:

Friedman discloses an image processing apparatus wherein said generation means generates the signature data by the use of a one way function, where the one way function is the encryption with a private key. (Column 4, lines 37-46)

In reference to claim 4:

Friedman discloses an image processing apparatus wherein said generation means generates the signature data by the use of a secret key cryptosystem. (Column 4, lines 37-46)

In reference to claim 5:

Friedman discloses an image processing apparatus wherein the confidential information relates to the image processing apparatus, where the confidential information includes the focusing distance of the camera lens system and range, and other characteristics stating where conditions in which the picture was taken. (Column 4, lines 57-66)

In reference to claim 6:

Friedman discloses an image processing apparatus wherein the confidential information relates to a user who uses the image processing apparatus, where the confidential information includes the GPS location where the user took his or her picture. (Column 9, lines 15-27)

In reference to claim 8:

Friedman discloses an image processing apparatus further comprising an image pickup unit for generating the digital image. (column 4, lines 30-45) The examiner notes that this is inherent to a digital camera.

In reference to claim 9:

Friedman discloses an image processing apparatus wherein said calculation means performs the predetermined calculation every time said image pickup unit generates the digital image. (column 8, lines 37-57)

In reference to claim 10:

Friedman discloses an image processing apparatus that is a digital camera. (column 4, lines 30-45)

In reference to claim 12:

Friedman discloses an image processing apparatus comprising:

- input means for inputting a digital image and signature data used for detecting the integrity of the digital image, where the input means are provided by the digital camera and the secure processor, and the intended use is for detecting the integrity of the digital image. (Column 4, lines 30-54)
- calculation means for performing a predetermined calculation using a digital image and confidential information, where the predetermined calculation is a digital hash of the image (Column 4, lines 34-36), and the confidential information is textual information added to the image including a unique image sequence number and the GPS location at which the image was taken. (Column 4, lines 55-66) & (Column 9, lines 15-28)
- detecting means for detecting the integrity of the digital image, with the use of the signature data and a result of the predetermined calculation, where the predetermined calculation is a digital hash, and the signature data is the encrypted hash (encrypted using a private key), and the authentication process detects the integrity of the digital image. (Column 4, lines 37-54)

Claim 21 is rejected for the same reasons as claim 1.

Claims 13, 22, 30 are rejected for the same reasons as claim 2.

Claims 14, 23, 31 are rejected for the same reasons as claim 3.

Claims 15, 24, 32 are rejected for the same reasons as claim 4.

Claims 25, 33 are rejected for the same reasons as claim 5.

Claims 26, 34 are rejected for the same reasons as claim 6.

Claim 28 is rejected for the same reason as claim 8.

Claim 29 is rejected for the same reasons as claim 12.

In reference to claim 16:

Friedman discloses an image processing apparatus wherein the confidential information relates to the unit for generating the signature data which is also the image processing apparatus unit, where the confidential information includes the focusing distance of the camera lens system and range, and other characteristics stating where conditions in which the picture was taken. (Column 4, lines 57-66)

In reference to claim 17:

Friedman discloses an image processing apparatus wherein the confidential information relates to a user who uses the unit for generating signature data which is also the image processing apparatus unit, where the confidential information includes the GPS location where the user took his or her picture. (Column 9, lines 15-27)

In reference to claim 20:

Friedman discloses an image processing apparatus wherein the image processing apparatus is a computer. (Column 4, lines 20-30)

While it may not be a computer in the traditional desktop computer sense, a computer to those of ordinary skill in the art are "generally regarded as a programmable electronic device that stores, processes, and receives data." (Merriam Webster's Collegiate Dictionary, 10th edition, "Computer")

A digital camera, receives data through the lens, processes the data through the authentication process, stores the data in memory, and is programmable by a user for simple settings, or the manufacturer who programmed the authentication algorithms into the processors.

In reference to claim 37:

Friedman discloses an image processing method comprising the steps of:

- performing a predetermined calculation using a digital image and confidential information, where the predetermined calculation is a digital hash of the image (Column 4, lines 34-36), and the confidential information is textual information added to the image including a unique image sequence number and the GPS location at which the image was taken. (Column 4, lines 55-66) & (Column 9, lines 15-28)
- generation means for generating signature data, using a result of the predetermined calculation, where the predetermined calculation is the digital hash, for use in detecting the integrity of the digital image. (Column 4, lines 37-46)
- externally outputting the digital image and the signature data, where the digital image and signature data are output to a digital system. (Column 4, lines 2-6)

- externally inputting the digital image and the signature data, where the digital image are input through the camera system, by taking a picture. (Column 3, lines 60-65)
- performing a second predetermined calculation using the digital image and the confidential information, where the second predetermined calculation is the checking hash, also produced from the digital image and the confidential information. (Column 6, lines 24-52)
- detecting the integrity of the digital image, using the signature data and a result of the second predetermined calculation, where the integrity is detected by comparing the first and second predetermined calculations, where the second predetermined calculation was produced by decrypting the signature data, and the comparison yields the result of whether the digital image had been modified or not. (Column 6, lines 24-52)

In reference to claim 38:

Friedman discloses an image processing apparatus comprising:

- calculation means for performing a predetermined calculation using a digital image and confidential information, where the predetermined calculation is a digital hash of the image (Column 4, lines 34-36), and the confidential information is textual information added to the image including a unique image sequence number and the GPS location at which the image was taken. (Column 4, lines 55-66) & (Column 9, lines 15-28)
- generation means for generating signature data, using an output of said calculation means, for use in determining whether the digital image had been modified. (Column 4, lines 37-46)

In reference to claim 39:

Friedman discloses an image processing apparatus comprising:

- input means for inputting a digital image and signature data used for determining whether the digital image has been modified, where the input means are provided by the digital camera and the secure processor, and the intended use is for detecting the integrity of the digital image. (Column 4, lines 30-54)
- calculation means for performing a predetermined calculation using a digital image and confidential information, where the predetermined calculation is a digital hash of the image (Column 4, lines 34-36), and the confidential information is textual information added to the image including a unique image sequence number and the GPS location at which the image was taken. (Column 4, lines 55-66) & (Column 9, lines 15-28)
- detecting means for determining with the use of the signature data and an output of said calculation means whether the digital image has been modified, where the signature data is the encrypted hash (encrypted using a private key), and the authentication process detects the integrity of the digital image. (Column 4, lines 37-54)

In reference to claim 40:

Friedman discloses an image processing method comprising the steps of:

- performing a predetermined calculation using a digital image and confidential information, where the predetermined calculation is a digital hash of the image (Column 4, lines 34-36), and the confidential information is textual information added to the image including a unique image sequence number and the GPS location at which the image was taken. (Column 4, lines 55-66) & (Column 9, lines 15-28)

- generation means for generating signature data, using a result of the predetermined calculation, where the predetermined calculation is the digital hash, for use in determining whether the image had been modified. (Column 4, lines 37-46)

In reference to claim 41:

Friedman discloses an image processing method comprising the steps of:

- inputting a digital image and signature data used for determining whether the digital image has been modified, where the digital image is input by the digital camera and the secure processor, and the intended use is for detecting the integrity of the digital image. (Column 4, lines 30-54)
- performing a predetermined calculation using a digital image and confidential information, where the predetermined calculation is a digital hash of the image (Column 4, lines 34-36), and the confidential information is textual information added to the image including a unique image sequence number and the GPS location at which the image was taken. (Column 4, lines 55-66) & (Column 9, lines 15-28)
- determining according to the signature data and a result of the predetermined calculation of said calculation means whether the digital image has been modified, where the predetermined calculation is the digital hash, and the signature data is the encrypted hash (encrypted using a private key), and the authentication process detects the integrity of the digital image. (Column 4, lines 37-54)

In reference to claim 42:

Friedman discloses an image processing method comprising the steps of:

- performing a predetermined calculation using a digital image and confidential information, where the predetermined calculation is a digital hash of the image (Column 4, lines 34-36), and the confidential information is textual information added to the image including a unique image sequence number and the GPS location at which the image was taken. (Column 4, lines 55-66) & (Column 9, lines 15-28)
- generating signature data, using a result of the predetermined calculation, where the predetermined calculation is the digital hash, for use in determining whether the image had been modified. (Column 4, lines 37-46)
- externally outputting the digital image and the signature data, where the digital image and signature data are output to a digital system. (Column 4, lines 2-6)
- externally inputting the digital image and the signature data, where the digital image are input through the camera system, by taking a picture. (Column 3, lines 60-65)
- performing a second predetermined calculation using the digital image and the confidential information, where the second predetermined calculation is the checking hash, also produced from the digital image and the confidential information. (Column 6, lines 24-52)
- detecting the integrity of the digital image, using the signature data and a result of the second predetermined calculation, where the integrity is detected by comparing the first and second predetermined calculations, where the second predetermined calculation was

produced by decrypting the signature data, and the comparison yields the result of whether the digital image had been modified or not. (Column 6, lines 24-52)

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 7, 11, 18, 19, 27,35, 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Friedman.

In reference to claim 7:

Friedman discloses an image processing apparatus but fails to state which digital format he uses in the apparatus.

The examiner takes official notice that digital images that are efficiently encoded or compressed are well known in the art. Examples of these efficiently encoded images are .JPEGS, or .gifs.

It would have been obvious to one of ordinary skill in the art at the time of invention to store the images in a highly efficient format, so that more images may be stored in less memory, allowing more pictures to be taken.

Claims 18, 27, 35 are rejected for the same reasons as claim 7.

In reference to claim 11:

Friedman discloses an image processing apparatus but fails to explicitly disclose an embodiment wherein the image processing apparatus is a scanner.

The examiner takes official notice that a scanner is a well known image processing apparatus, and like a digital camera, also equipped with the means to acquire images of certain objects. Additionally scanners may also attach to a computer or external system in the same way as a digital camera, such as through the use of a USB port.

It would have been obvious to one of ordinary skill in the art at the time of invention to apply the image authentication mechanism of Friedman and apply it for use in a scanner given the benefit of being able to authenticate images acquired by scanner and assure that scanned images have not been modified.

In reference to claim 19:

Friedman discloses the image processing method of claim 29.

The examiner takes official notice that the step of displaying the results of a test, such as displaying the integrity test of Friedman on a display unit, such as a monitor is well known in the art.

It would have been obvious to one of ordinary skill in the art to display the results of the integrity test of Friedman on a display unit, given the strong need to see the results of the data and actually know if the image had been properly authenticated or not.

Claim 36 is rejected for the same reasons as claim 19.

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas M Ho whose telephone number is (703)305-8029. The examiner can normally be reached on M-F from 8:30am – 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached at (703)308-4789. The fax phone numbers for the organization where this application or proceeding is assigned are (703)746-7239 for regular communications and (703)746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)306-5484.

TMH

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

December 4th, 2003